Navy and Marine Corps Intranet Certification and Accreditation

Mr. Bob Turner, Booz Allen Hamilton Senior Consultant

NMCI IA Lead

NAVNETWARCOM Information Assurance Division

(757) 417-6776/DSN 537-6776

*Robert.Turner@netwarcom.navy.mil*

Our Goal……Protecting the Navy's Networks At Sea and On Shore

What are we protecting?

- DOD Information
  - Classified Info
  - Privacy Act Info
  - Sensitive but Unclassified/Nuclear In
  - FOUO (For Official Use Only)
- Systems
  - C4 (Command, Control, Communication & Computer) Systems
  - POR (Program of Record) Systems
- Networks
  - NIPRNET (Unclassified)
  - SIPRNET (Classified)
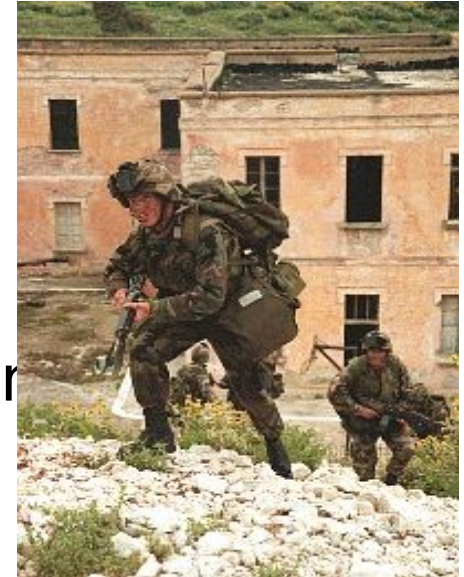
What are we protecting from?

- Insider Threat (Often under-estimated)
  - Disgruntled personnel
  - Unintentional actions of user
  - Trusted insider
- Hacker/Cracker
- Malicious Code/Viruses/Worms
- State Sponsored CNA (Computer Network Attack)
- DOS (Denial of Service) Attacks
  - Self imposed
  - Deliberate actions of others

NETWARCOM IA Strategy...Focus Areas

- NETWARCOM Strategy is Navy Strategy and aligns with DOD strategy
  - Navy DAA (Designated Approval Authority)
- CND (Computer Network Defense)
  - Protect, Detect, React and Recover
- DiD (Defense in Depth)
  - CNDiD
- Certification and Accreditation
- OPSEC (Operations Security)
- Situational Awareness, Network Health & Training
- Scope includes
  - NMCI (Navy/Marine Corps Internet)
  - BLII (Base Level Information Infrastructure)
  - IT21 (ISNS)

Moving from "Reactive" to "Proactive""

Defense-in-Depth:
It's more than just technology

Defense-in-depth

People

Operations
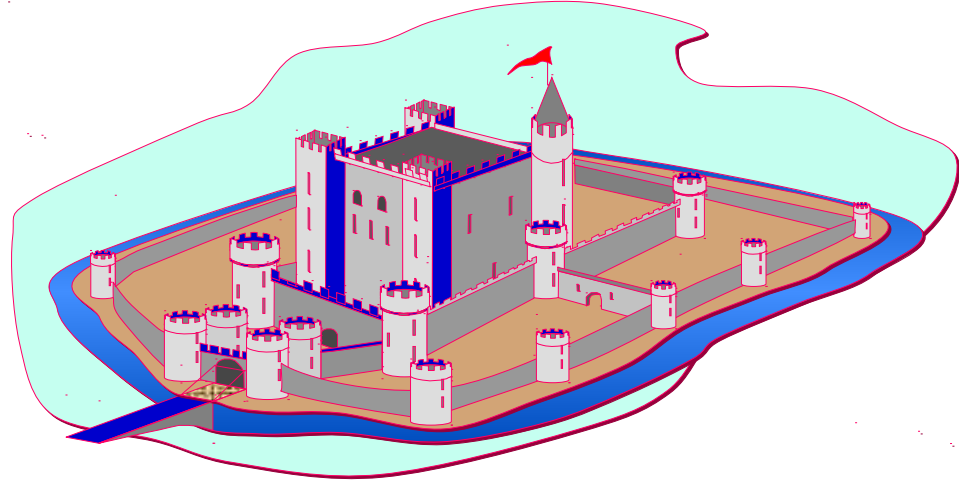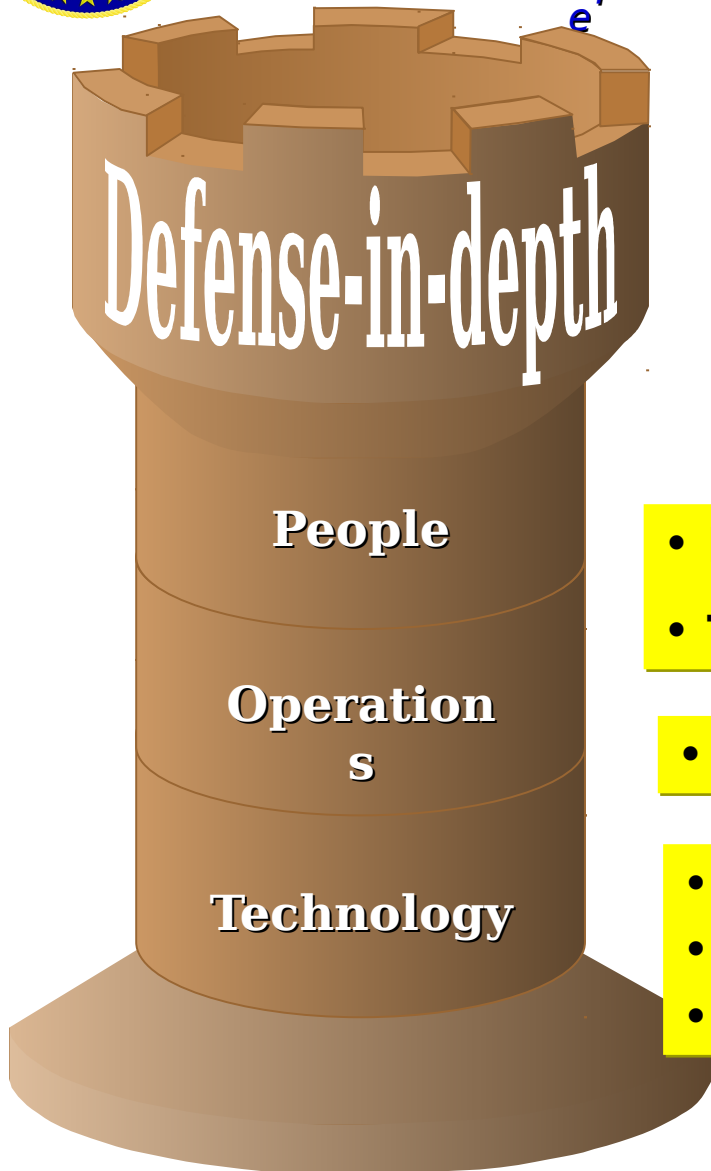
Technology

- **Right people in the right job**
- **Training, Training, Training**

- **Tactics, Techniques, and Procedures**

- **Hardened infrastructure**
- **Layered Protection**
- **Right DiD tool/technology in the right layer**

Mission *People* *Capability*

- Core Technical Skills on Staff

  - User → IA Implementer

- Technical Depth in Partnership Organizations

- Management of ISSMs throughout the Fleet, Depth to the Deckplate

Train, Train, Train

- IAVM Process – an Enabler to Success
- Red Team Operations/Assessments
- Active and Passive Monitoring Tools
  - Securify
  - Harristat
  - ISS
- Information Conditions (INFOCONs)

Tactics, Techniques, and Procedures

Mission *People* *Capability*

- As new technologies emerge, security must be built in from the ground up using enclave/boundary layers.

    Local Network   NMCI Deployment

    BLII OCONUS Upgrades   IT-21 Fielding

    Coalition Force Integration   FORCEnet

    Next Generation Network Development

    Joint Command and Control Capabilities

Right Technology at the Right Layer

Defense In Depth

- Layers of Protections
  - User Level
    - Authentication
      - User Certificates (PKI)
    - Training (CNVA)/OLS
  - Boundary Level
  - Enterprise Level
    - Filters/Routers
    - Encryption
    - Firewalls
    - Intrusion Detection
  - Transport Encryption

Why NMCI?

- Purchasing a "Service"
  - SLA (Service Level Agreement) performance
- Consolidated Infrastructure
  - Improves security posture for Navy and identifies all networks
- Enhanced network security
  - Enables Configuration Mgmt
  - Enables quick response capability
  - Legacy applications quarantined
- Global Network Administration
  - Security patches pushed
- Technology refresh every 3 years

Certification and Accreditation

- DITSCAP = DOD Information Technology Security Certification and Accreditation Process

- Designated Approval Authority (DAA)
  - Focus for industry is Developmental DAA
  - Active Involvement
  - Risk Management

- Program Manager (PM)
  - Ensures Security Design

- Certification Authority/Agent (CA)
  - Reviews package/supports PM in design and verification

C&A 101

- Certification = "Comprehensive evaluation of technical and non-technical security features…"

- Accreditation = "Formal declaration by DAA that system is approved to operate in a particular security mode using prescribed safeguards at an acceptable level of risk…"

- Standards
  - International Common Criteria for INFOSEC Technology Evaluation
  - NSA/NIST/NIAP
  - NIST FIPS

C&A Process

- Levels of assurance
  - Basic, Medium, High

- Tools
  - Checklists
  - Network Vulnerability Tool
  - Common Criterial EAL

- System vs. Component

- "Type" vs. Site
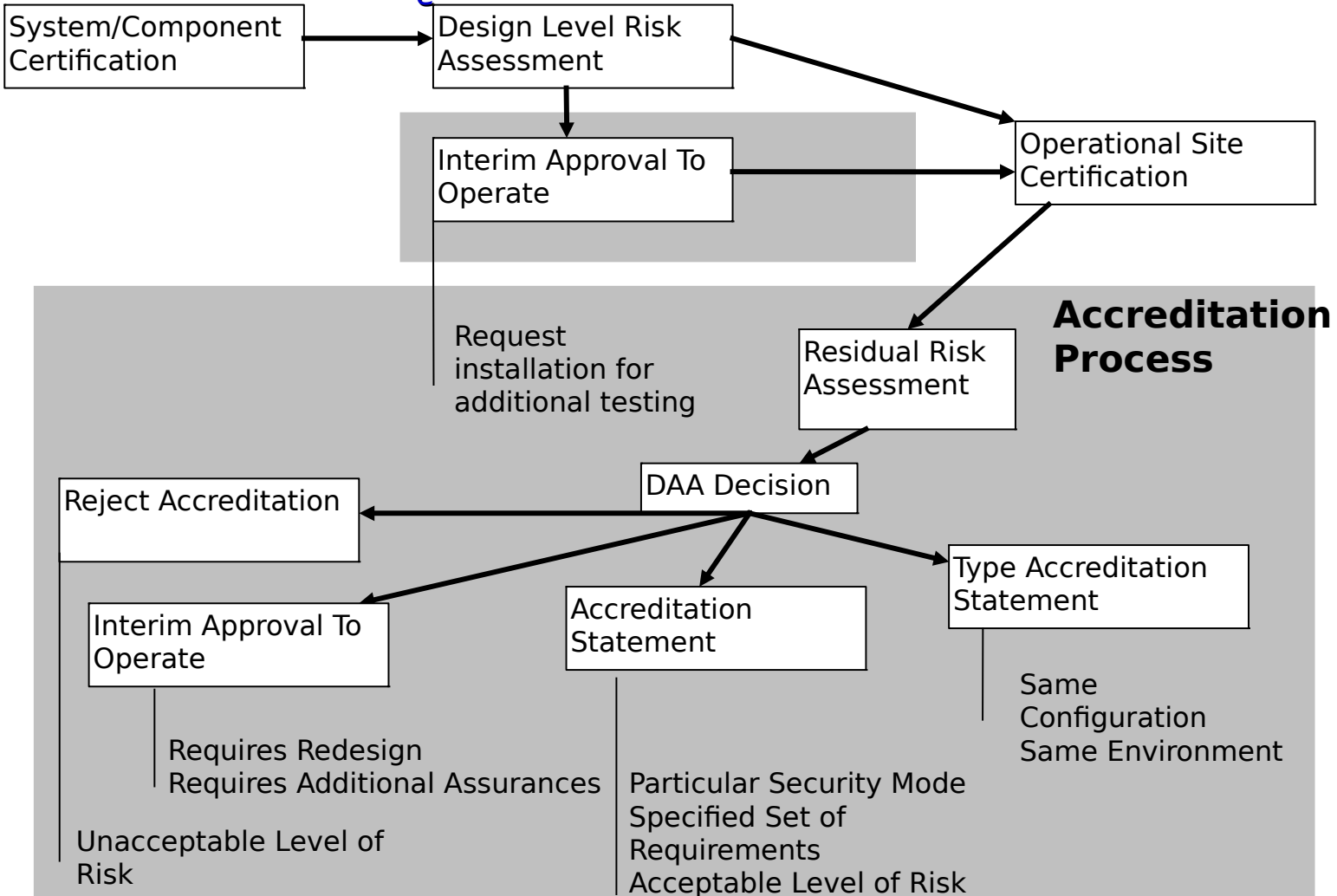
- Operational Environment Certification

14

- Approach depends on system and implementation

- Risk Assessment
  - Technical
  - Non-Technical
  - Acceptable Level of Risk

- Accreditation Statement
  - System, Type, Site, POR

C&A Process

System/Component Certification → Design Level Risk Assessment

Design Level Risk Assessment → Interim Approval To Operate

Design Level Risk Assessment → Operational Site Certification

Interim Approval To Operate → Operational Site Certification

Request installation for additional testing

Operational Site Certification → Residual Risk Assessment

Accreditation Process

Residual Risk Assessment → DAA Decision

DAA Decision → Reject Accreditation

DAA Decision → Interim Approval To Operate

DAA Decision → Accreditation Statement

DAA Decision → Type Accreditation Statement

Interim Approval To Operate
Requires Redesign
Requires Additional Assurances
Unacceptable Level of Risk

Accreditation Statement
Particular Security Mode
Specified Set of Requirements
Acceptable Level of Risk

Type Accreditation Statement
Same Configuration
Same Environment

16

C&A References

- **NSTISSI 4009** - National Information Systems Security (INFOSEC) Glossary, January 1999
- **NSTISSI No 4011** - National Training Standard for Information Systems Security (INFOSEC) Professionals
- **NSTISSP Fact Sheet 11** – National Information Assurance Acquisition Policy, January 2000
- **Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8519** "Department of Defense Global Information Grid Information Assurance, June 2000
- **DODInst 5200.40** Department of Defense Information Technology Security Certification and Accreditation Process
- **SECNAV 5239.3** – Department of the Navy Information Systems Security (INFOSEC) Program. (CH-1 dated 17 Jan 1997) and 14 July 95.
- **OPNAVINST 5239.1B** - Navy Information Assurance (IA) Program, 9 Nov 1999.
- **DoN IA Publication 5239 (Series)** - Information Assurance (IA)
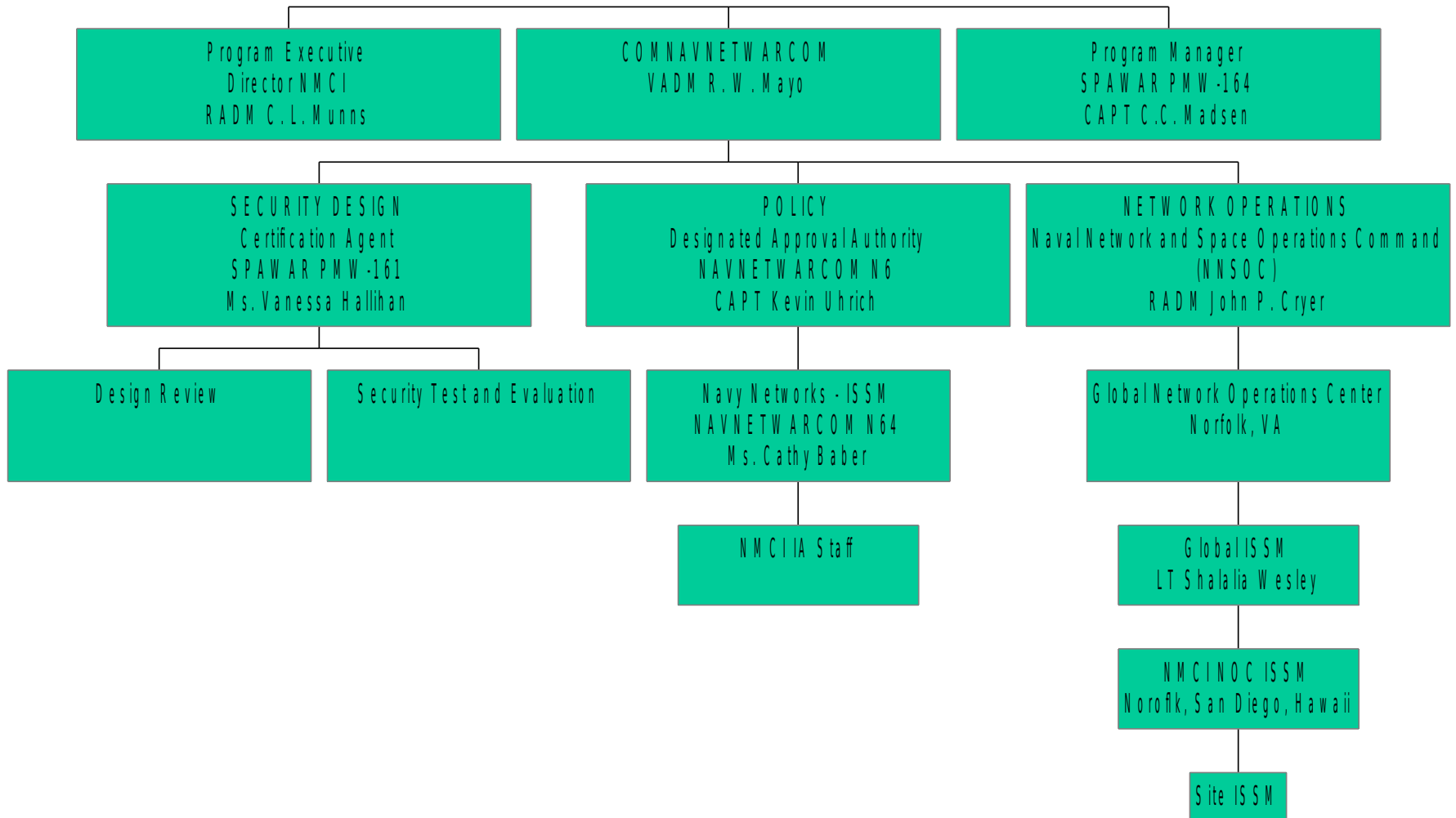
- Sponsorship (requirements analysis)

- Documentation (network architecture)

- Vulnerabilities (network/component)

- Self Diagnosed Risk

- Adequate Physical/Administrative Controls

- Conceptual Risk Assessment (CA endorsement)

- DAA Accreditation (IATO/ATO)

NMCI Security Organization

Mission *People* *Capability*

```
┌─────────────────────┐   ┌─────────────────────┐   ┌─────────────────────┐
│  Program Executive  │   │  COMNAVNETWARCOM   │   │   Program Manager   │
│   Director NMCI     │   │   VADM R.W. Mayo    │   │   SPAWAR PMW-164    │
│  RADM C.L. Munns    │   │                     │   │  CAPT C.C. Madsen   │
└─────────────────────┘   └─────────────────────┘   └─────────────────────┘
```

SECURITY DESIGN
Certification Agent
SPAWAR PMW-161
Ms. Vanessa Hallihan

POLICY
Designated Approval Authority
NAVNETWARCOM N6
CAPT Kevin Uhrich

NETWORK OPERATIONS
Naval Network and Space Operations Command
(NNSOC)
RADM John P. Cryer

Design Review

Security Test and Evaluation

Navy Networks - ISSM
NAVNETWARCOM N64
Ms. Cathy Baber

Global Network Operations Center
Norfolk, VA

NMCI IA Staff

Global ISSM
LT Shalalia Wesley

NMCI NOC ISSM
Noroflk, San Diego, Hawaii

Site ISSM

C&A Points of Contact

NNWC

Mr. Bob Turner

(757)417-6776 Ext 2
Robert.Turner@netwarcom.navy.mil

Mr. Larry Downs

(757)417-6719 Ext 3 Larry.Downs@netwarcom.navy.mil

LCDR John Ross

(757)417-6776 Ext 1 John.Ross@netwarcom.navy.mil

SPAWAR

PMW-161 CDR John Sicklick

(619)524-7340 John.Sicklick@navy.mil

Questions?